

Amendments

In accordance with 37 CFR §1.121, please amend the above-identified application as set forth below.

Amendments to the Claims:

Please amend the claims as set forth below.

18. (Currently Amended) A method for peer-to-peer messaging between network resources comprising:

obtaining, by a first arbiter, a first output of a first process;
parsing information within the first output into a first set of text files;
writing the first set of text files into a text file in a scratch space;
detecting, by a second arbiter of a second process, the text file;
reading, by the second arbiter, the text file received within the scratch space to find a
digital signature within the text file;

comparing the digital signature to the contents of the text file to determine whether the
digital signature is valid;

moving the text file to a queue designated for improper files on determining that the
digital signature is invalid; and

processing the text file on determining that the digital signature is valid.

19. (Original) A method in accordance with claim 18 further comprising: comparing the digital signature with signatures in a list in a database on determining that the digital signature is valid,

wherein the comparison is made to determine whether there is permission to transmit the text file.

20. (Original) A method in accordance with claim 18 wherein processing the text file comprises processing according to one of an independent rule set of an arbiter that reads the text file and instructions within the text file.

21. (Currently Amended) A method for peer-to-peer messaging between network resources comprising:

obtaining, by a first arbiter, a first output of a first process;

parsing information within the first output into a first set of text files;

writing the first set of text files into a text file in a scratch space;

detecting, by a second arbiter of a second process, the text file;

reading, by the second arbiter, the text file to find at least one portion of the text file and

to find a digital signature within the portion, wherein the portion is designated for processing;

comparing the digital signature to the contents of the portion of the text file to determine whether the digital signature is valid;

moving the portion of the text file to a queue designated for improper portions of files on determining that the digital signature is invalid; and

processing the portion of the text file on determining that the digital signature is valid.

22. (Original) A method in accordance with claim 21 further comprising: comparing the digital signature with signatures in a list in a database on determining that the digital signature is valid,

wherein the comparison is made to determine whether there is permission to transmit the portion of the text file.

23. (Original) A method in accordance with claim 21 wherein processing the portion of the text file comprises processing according to one of an independent rule set of an arbiter that reads the text file and instructions within the portion of the text file.

24. (Original) A method for peer-to-peer messaging between network resources comprising:

obtaining, by a first arbiter, a first output of a first process; parsing information within the first output into a first set of text files;

writing the first set of text files into a first text file in at least one of a first scratch space and a second scratch space;

detecting, by a second arbiter of a second process, the first text file; reading, by the second arbiter, the first text file;

and performing an independent operation on the first text file based on rules in the second arbiter to obtain a second output.

25. (Currently Amended) A method in accordance with claim 24 wherein performing the independent operation ~~comprises~~ is selected from the group of operations consisting of (a) referring to at least one of external databases, external data files, and external objects to perform the independent operation, (b) finding a digital signature within the first text file and comparing the digital signature to the contents of the first text file to determine whether the digital signature is valid, and (c) finding a digital signature within a portion of the first text file designated for

processing and comparing the digital signature to the contents of the designated portion of the first text file to determine whether the digital signature is valid, and (d) any combination thereof.

26. (Original) A method in accordance with claim 24 further comprising writing the first output to at least one of the first scratch space and other scratch spaces.

27. (Original) A method in accordance with claim 24 further comprising: obtaining, by a third process, the second output; parsing information within the second output into a second set of text files; writing at least one of the files in the second set into a third text file in a third scratch space; detecting, by a third arbiter, the third text file; reading, by the third arbiter, the third text file; and performing an independent operation on the third text file based on rules in the third arbiter to obtain a third output.

28. (Original) A method in accordance with claim 24 further comprising formatting, by the first arbiter, information available to the first arbiter.

29. (Original) A method in accordance with claim 28 further comprising sending, by the first arbiter, the information to the second process via an interface.

30. (Original) A method in accordance with claim 29 wherein sending, by the first arbiter, the information comprises sending, by the first arbiter, an image to display the image along with a document of the second process.

31. (Original) A method in accordance with claim 29 wherein sending, by the first arbiter, the information comprises sending, by the first arbiter, an image of a check to display the image along with a document of the second process.